STATE OF ALABAMA

Information Technology Standard

Standard 670-01S2: Risk Mitigation

1. INTRODUCTION:

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission.

2. OBJECTIVE:

Establish the requirements for risk mitigation for the State of Alabama computing environment.

3. SCOPE:

These requirements apply to all users (State of Alabama employees, contractors, vendors, and business partners) of any State-managed information system resources.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) Special Publication 800-30: Risk Management Guide for Information Systems, the State of Alabama organizations shall utilize the following risk mitigation options and methodologies:

4.1 RISK MITIGATION OPTIONS

Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level

Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified)

Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability (e.g., use of supporting, preventive, detective controls)

Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls

Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability

Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

4.2 RISK MITIGATION METHODOLOGY

Prioritize Actions. Based on the risk levels presented in the risk assessment report; the implementation actions will be prioritized. When allocating resources, top priority will be given to risk items with a High risk ranking first; Medium risk ranking second; then the Low risk ranking items. These High risk vulnerability/threat pairs will require immediate corrective action.

Evaluate Recommended Control Options. During this step, the feasibility of the recommended control options shall be analyzed. The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific State organization and their IT system. The goal is to select the most appropriate control option for minimizing risk.

Conduct Cost-Benefit Analysis. To aid management in making a decision on what risk mitigation option to employ, a cost-benefit analysis will be conducted.

Select Control. On the basis of the results of the cost-benefit analysis, management will determine the most cost-effective control(s) for reducing risk to the affected IT system or network. The controls selected should combine technical, operational, and management control elements to ensure adequate security for the IT system, network and organization.

Assign Responsibility. Identify personnel who have the appropriate expertise and skill-sets to implement the selected control and assign responsibility. If in-house personnel are not available, then contractors may be used.

Develop a Safeguard Implementation Plan. A safeguard implementation plan will be developed. The plan should, at a minimum, contain the following information:

- Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
- Recommended controls (output from risk assessment report)
- Prioritized actions (with priority given to items with High risk levels
- Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
- Required resources for implementing the selected planned controls
- Lists of responsible teams and staff
- Start date for implementation
- Target completion date for implementation
- Maintenance requirements

Implement Selected Control(s). Depending on the specific situations, the implemented controls may lower the risk level but not eliminate the risk entirely. All residual risk will be documented in a Residual Risk Report and provided to management.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 670-01: Risk Management

6.2 RELATED DOCUMENTS

Information Technology Standard 670-01S1: Risk Assessment

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/12/2006	